EXHIBIT 29

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,	:	
	:	
PLAINTIFFS,	:	
vs.	:	DOCKET NUMBER
	:	1:17-CV-2989-AT
BRAD RAFFENSPERGER, ET AL.,	:	
	:	
DEFENDANTS.	:	

TRANSCRIPT OF HEARING ON PRELIMINARY INJUNCTION PROCEEDINGS

BEFORE THE HONORABLE AMY TOTENBERG

UNITED STATES DISTRICT JUDGE

JULY 25, 2019

10:10 A.M.

VOLUME 1 OF 2

MECHANICAL STENOGRAPHY OF PROCEEDINGS AND COMPUTER-AIDED TRANSCRIPT PRODUCED BY:

OFFICIAL COURT REPORTER: ***SHANNON R. WELCH, RMR, CRR***
2394 UNITED STATES COURTHOUSE
75 TED TURNER DRIVE, SOUTHWEST
ATLANTA, GEORGIA 30303
(404) 215-1383

I N D E X T O P R O C E E D I N G S

WITNESS	PAGE
SANFORD MERRITT BEAVER	
Cross-Examination by Mr. Cross	21
Cross-Examination by Mr. Brown	49
Direct Examination by Mr. Russo	54
Recross-Examination by Mr. Cross	61
Examination by The Court	63
MICHAEL LEON BARNES	
Cross-Examination by Ms. Bentrott	73
Cross-Examination by Mr. Brown	81
Direct Examination by Mr. Russo	96
Examination by The Court	105
Recross-Examination by Ms. Bentrott	106
TERI ADAMS	
Direct Examination by Mr. Brody	109
Cross-Examination by Mr. Lake	111
AMBER MCREYNOLDS	
Direct Examination by Mr. Brown	116
Voir Dire Examination by Mr. Belinfante	120
Direct Examination (Continued) by Mr. Brown	124
Cross-Examination by Mr. Belinfante	138

(...cont'd...)

WITNESS		PAGE
	Cross-Examination	
	by Ms. Burwell	147
	Redirect Examination	
	by Mr. Brown	157
	Recross-Examination	
	by Mr. Belinfante	159
MICHAEL LEON BARNES		
	Reexamination	
	by The Court	161
	Redirect Examination	
	by Mr. Russo	172
	Recross-Examination (Further)	
	by Mr. Brown	172
	Reexamination (Further)	
	by The Court	173
	Recross-Examination (Further)	
	by Mr. Brown	174
JASMINE CLARK		
	Direct Examination	
	by Mr. Powers	175
	Cross-Examination	
	by Mr. Lake	182
SARA LECLERC		
	Direct Examination	
	by Mr. Brown	190
	Cross-Examination	
	by Mr. Lake	194
KATHY POLATTIE		
	Direct Examination	
	by Mr. Powers	196
	Cross-Examination	
	by Mr. Lake	199
THERESA PAYTON		
	Cross-Examination	
	by Mr. Cross	205

(...cont'd...)

WITNESS	PAGE
Direct Examination by Mr. Tyson	238
Recross-Examination by Mr. Cross	273
Redirect Examination by Mr. Tyson	280
Examination by The Court	283
Recross-Examination (Further) by Mr. Cross	292
Redirect Examination (Further) by Mr. Tyson	294
MICHAEL SHAMOS, PH.D. (Videotaped Deposition)	303
* * *	
CERTIFICATE	313

A. No.
Q. Well, you're not taking the position that it is different from the Cobb County one -- the structure; right?
A. The table names are the same in the Cobb County database as what we use in Georgia's GEMS database.
Q. The structure is the same? If you were to put those screenshots side-by-side, they are virtually identical, are they not, sir?

MR. RUSSO: Objection, Your Honor. They haven't authenticated this Cobb County database.

THE COURT: Well, he says he has now looked at it. So that is -- that is an adequate foundation.

Q. **(BY MR. CROSS)** The tables themselves are also virtually identical if we look at them side-by-side; right, sir?
A. From what I can tell, the table names are the same.
Q. You retained a company called Fortalice to do cybersecurity assessments in 2017 and 2018; right?
A. Yes.
Q. And the networks that they examined for that included elections-related networks; correct, sir?
A. Yes.
Q. The first assessment that they produced was in October of 2017; right?
A. Yes.
Q. And they identified 22 -- 22 security risks in the

networks that they examined; right?
A. Yes.
Q. They then completed another assessment on November 30 of 2018; correct?
A. Correct.
Q. And you personally requested that assessment, did you not, sir?
A. I request them every year since I have been employed by the Secretary of State.
Q. So as of November 30 of last year, as of that assessment, only 3 of the 22 risks identified in 2017 had been remediated; right?
A. I don't know that that is true. I'm not sure where you got that information.
Q. Have you not read -- well, let me take a step back.
Do you know who Theresa Payton is?
A. Yes.
Q. And she actually heads up Fortalice, the company that you engaged; right?
A. Yes.
Q. Have you read the declaration that she submitted in this case?
A. No.
Q. Well, she states, of the risks outlined in the 2017 report, Fortalice found that as of the November 2018 assessment

three risks had been remediated with compensating controls and another three were in process of being fixed.

You didn't read that before?

A. No.

Q. Do you have any reason to think that Ms. Payton who oversaw the risk assessment is wrong?

A. I would have to review what she said. I don't believe that we only covered three. In fact, I'm confident that we've covered more than three. And maybe her understanding of what was done wasn't clear.

Q. So the Court cannot rely on Ms. Payton's representations about the risks associated with your system, right, because she may not understand?

A. No, that is not true.

Q. Well, you just represented --

A. The risks that were identified in '17 weren't necessarily the risks that were identified in '18.

Q. I understand. I'm asking you a simple question, Mr. Beaver. I need you to listen and answer my question. Okay?

Are you representing to the Court that it cannot take as fact Ms. Payton's representation that 19 of the 22 risks identified in 2017 had not yet been remediated as of November 30 of 2018? Can she not take that as fact?

A. I need to understand her measurement because remediate may

be completely fixed versus in process or partially fixed.

Q. You are aware that there was an election in the state on November 6 of last year; right?

A. Yes.

Q. So at least according to Ms. Payton, at the time that the state went through an election in which almost 4 million voters voted including at the highest levels in the state government for the governor, at least according to her, 19 of 22 significant risks -- she characterized them as significant -- were still outstanding as of the election; right?

A. Okay.

Q. But you just don't know one way or the other as you sit here as to whether that is right; correct?

A. I would have to see her document.

Q. Some of the risks that she identified, the first one, Number 1, the most significant was what she called widespread local administrative rights.

Do you recall that?

A. Yes.

Q. What that meant was that every Georgia Secretary of State user was granted administrative rights on their work stations?

A. Yes.

Q. Correct? What that means is they don't just log in and use the computer? With administrative rights, every single user has the ability to download software if they want to to

that computer; right?
A. Yes.
Q. Administrative rights enables them to affect the programming of that computer; right?
A. Correct.
Q. You're aware, as Fortalice pointed out, that this created a significant risk of malware infecting the networks that they were examining; correct?
A. Are we talking about the 2017?
Q. I'm talking about the risk assessment that was done in 2017.
A. Yes.
Q. And, again, we have established the networks that she was examining -- Fortalice was examining included election-related networks; right?
A. Correct.
Q. In fact, Fortalice pointed out that the risk was particularly significant for the Georgia Secretary of State because not only did every user have administrative rights on their own work station but they had administrative rights for every work station in the Secretary of State's office.
Do you recall that?
A. Yes.
Q. Meaning that someone with access to a single work station had administrative rights to every other work station and could

do all the things we just talked about; right?
A. In 2017, that was correct. That has been remediated in. 2017.
Q. So you know that that was remediated, but you don't know about the other 19 that Ms. Payton said were not remediated as of the election?
A. I would have to see them.
Q. Another vulnerability that Ms. Payton and her team found was that the Georgia Secretary of State relied on legacy systems and software that were no longer supported or receiving security patches even when new vulnerabilities were identified; right?
A. Correct.
Q. And this created a significant risk that a hacker could easily exploit unpatched devices, which is what you were using; right?
A. Correct.
Q. Fortalice even found security --
A. You didn't ask me whether we had remediated it.
Q. I'll get there.
A. Okay.
Q. Fortalice even asked -- I'm sorry. Fortalice even found significant cybersecurity risks with the voter registration database in Georgia; right?
A. Can you repeat that, please?

A. You mean one through ten? Is that what you're talking about?

Q. Yes. At the bottom of the page.

A. Yes.

Q. Number 10 is lack of security controls for PCC, Inc.; right?

A. Yes. That is in the semi likely row.

Q. Right. That is not what I asked you.

A. Okay. I'm just verifying where I'm at.

Q. Lack of security controls for PCC, Inc., is Number 10. We're agreed on that; right?

A. Yes.

Q. Okay. And Number 10 corresponds to the security risks with the voter registration database because PCC is the company that owns and operates the voter registration database; right?

A. At the time, yes.

Q. And ten, if we look under the columns of significant, is to the far right in the risk heat map, so it is in the significant column of risk; right?

A. Yes. And it is in the row -- what is the row?

Q. Mr. Beaver, one of the concerns that was noted was the overarching concern of the lack of control and oversight that the state exercised over the registration database at the time.

Do you recall that?

A. Yes.

Q. And Fortalice urged you in October of 2017 to require the vendor, PCC, to conduct certain tasks and update its security; correct?

A. Correct.

Q. And then four months later in February of 2018, there was another assessment by Fortalice; right?

A. Yes.

Q. And at that point, they identified 15 security risks just with PCC with the voter registration database? Do you recall that?

A. I recall there are two different assessments that assessed different data centers. So the assessments of one do not apply to the other.

Q. So the assessments in February of 2018 were different additional risks with the voter registration database beyond what was identified four months earlier; right?

A. They are separate.

Q. Separate? 15 more?

A. We had an assessment of one data center where we have some applications running. We had an assessment of another data center where the election system is running. The election system is not in the first assessment.

Q. So the election system is in the second assessment where Fortalice identified in February of 2018 15 security risks; correct?

A. Is that this report? That is not this report.
Q. That is the February 2018 report. You don't recall that?
A. I do recall the February one. But I don't remember the count.
Q. So you need to see that too?
A. That would probably be good.
MR. CROSS: Your Honor, we'll mark this as Exhibit 2.
Q. **(BY MR. CROSS)** Mr. Beaver, you now have in front of you what is the February 2018 risk assessment that was done by Cloudburst and Fortalice; right?
A. Yes.
Q. As you pointed out, this one as you can see in the first sentence in Exhibit 2 indicates that they conducted a vendor cyber risk assessment on PCC Technology, Inc., again the company that owns and operated at least as of this time the voter registration database; correct?
A. Correct.
Q. And if you come to the second paragraph, do you see they reported Cloudburst Security suggests remediating the 15 identified security risks included in this report? Do you see that?
A. Yes.
Q. Does that refresh your recollection that as of February of 2018 your independent security vendor identified 15 risks that needed to be remedied?

A. Yes.
Q. In the November 2018 assessment, Fortalice did not look at PCC at all again; right? Do you remember you put that outside of scope?
A. Yes. It is a different data center.
Q. Are you aware of any attempt to hack a Georgia voter registration database around the time of the November 6 election last year?
A. It wasn't a database -- I mean, the voter registration database. It was the My Voter page.
Q. Which includes voter registration information; right?
A. It is a feeder that pulls data from that.
Q. Right. The My Voter page has access -- the data moves back and forth between that and the voter registration database?
A. Not back and forth. It is a one-way transfer, meaning the voter registration system feeds an extract of the database to My Voter page. So if anything happens in My Voter page, it has no impact -- cannot have any impact on the voter registration system. It is an isolated system for security purposes.
Q. In the November 2018 assessment, Fortalice made 20 additional -- beyond the reports we have looked at before, made 20 additional recommendations to the Secretary of State to improve cybersecurity; right?
A. Yes.

A. Security is not a --
Q. Yes or no. That did not appear in your declaration?
A. It did not appear.
Q. You go on in that same sentence as an example of one of the ways you protect the system -- you say, including conducting regular cyber assessments with penetration testing; right?
A. Yes.
Q. So you were representing to the Court that penetration testing is one of the ways that you confirm that your system is secure; right?
A. That is one of the ways.
Q. In the October 2017 assessment, again less than a year before your August 2018 declaration to the Court, Fortalice actually conducted one of those penetration tests; correct?
A. Yes.
Q. And it was successful? They penetrated the network, didn't they, sir?
A. They -- not the election system network. They penetrated the Secretary of State data center, which does not have the election system in it.
Q. They penetrated --
A. There are two different data centers I said earlier, the one at the Secretary of State's office which holds our corporations database, our professional licensing database, our

website, but does not contain the elections -- the voter registration system.

The system they penetrated was the one from the Secretary of State's data center. That was not the election system.

Q. Is the answer to my question yes, they did a penetration test, like you represented to the Court, that allowed them to penetrate some aspect of the Secretary of State's network? That is true; right, sir?

A. That is very true.

Q. And, in fact, the penetration enabled them to obtain domain administrator rights on the network that they penetrated; correct?

A. Correct.

Q. And we've talked about the expansive abilities of administrator rights already. That is what they obtained; right?

A. Correct.

Q. In fact, they point out they were able to gain access to network security systems? That was one of the things they identified; correct?

A. Correct.

Q. They point out that they were able to review the enterprise architecture and system configurations; correct?

A. Correct.

Q. And so when you represented to the Court that one of the

Q. The internal memory of the DRE voting machines themselves has never been tested or checked in any way; is that correct?

A. The internal memory -- the election files that are collected after each election, in some cases the county may have to access that file and bring it forward, if something happened to a memory card that had been previously in use for an election.

But has there been an inspection of that by the state? No.

Q. Is it -- it is still part of your practice to load files from the GEMS server on to a USB drive and to insert that drive into a Secretary of State public computer; correct?

A. That is correct.

Q. That computer is connected to the internet; right?

A. The Secretary of State's computer, yes.

Q. And after inserting that USB into the internet-facing computer, you will insert it back into the GEMS server; right?

A. Only after it is reformatted on the public computer after we have moved the file from the GEMS computer to the public computer for distribution to the county, particularly like a PDF file or reports that the county may need. After that file has been moved over to the public side, the USB drive that has been inserted into the public computer is then reformatted.

Q. And then reinserted back into the GEMS server?

A. After it is reformatted on the public, it is then at a

later point in time inserted back into the private system.

Q. Thank you. I would like to hand you what we'll mark as Exhibit 4 -- Exhibit 4.

MS. BENTROTT: And for the record, this is Senate findings -- a summary of Senate findings called Russian Targeting of Election Infrastructure During the 2016 Election, Summary of Initial Findings and Recommendations, dated May 8, 2018.

Q. **(BY MS. BENTROTT)** And you can see in the section on the first page summary of initial findings the first bullet reads, at least 18 states had election systems targeted by Russian-affiliated cyber actors in some fashion.

Do you see that finding?

A. I do.

Q. And in the second bullet, it says almost all of the states that were targeted observed vulnerability scanning directed at their Secretary of State websites or voter registration infrastructure.

Do you see that finding as well?

A. I do.

Q. Neither of these findings has changed your operations in any way; correct?

A. That is correct.

Q. You testified in your deposition that you weren't aware of any current or previous lapses in security in Georgia's voting

Q. And if you -- but to sort of cut to the chase, your office provides the programming and configuration for GEMS databases and for the ballots for a vast majority of the elections in Georgia; correct?

A. That is correct.

Q. And that would include all county elections?

A. That is correct.

Q. And all municipal elections when the municipality is having the Secretary of State either directly or through the county program and configure its database; correct?

A. The relationship is between the municipality and county. That is where that is governed. The Secretary of State -- we provide support for election ballot building for county elections offices. If county elections offices then contract with municipalities to execute the municipality election, then the Secretary of State's office through my division is building the database to provide to the county for that purpose.

Q. Are you familiar with the state's contract with -- ES&S's contract for ballot building support services?

A. I am.

Q. Mr. Barnes, what does ES&S do pursuant to that contract?

A. They assist my division in constructing the GEMS databases that are used within county elections.

Q. And so the state is outsourcing the building of the ballots; is that right?

A. We are using ES&S as a contractor to help us assist in that production.

Q. And I believe the contract for 2019 is for $150,000; is that right?

A. I believe that is correct, yes.

Q. How many full-time people is that from ES&S that are actually working on Georgia ballots?

A. I believe ES&S has three individuals that work solely on Georgia election databases.

Q. And that would be in addition to the individuals in your office?

A. That would be in addition to the individuals in my office, yes.

Q. Okay. And so does ES&S actually sit in your office and do this ballot building work?

A. They do not.

Q. Where do they do their ballot building work?

A. They do their ballot building work within their own purviews. We provided to ES&S when this contract was initially put together specifications on how that hardware must be configured, also with a specific image of build for that specific unit that they would be using to construct those databases.

Q. So -- and where is this done? Omaha?

A. No. It is all done within the State of Georgia. It is

all done within -- I believe the individuals work from home.
Q. So we have individuals from an outside contractor working at home on their own PCs on Georgia's GEMS databases, which program the ballots for all of Georgia's elections; is that correct?
A. We have three individuals, two of whom were previously employees of mine at the Center for Election Systems with over a decade's experience in building GEMS databases. And then the third individual is a former county elections official from Cobb County with over 25 years of experience in Georgia elections.
Q. I understand their experience. But they are at home working on their laptop, I guess, designing --
A. It is not a laptop.
Q. Or a PC. It is a desktop; right?
A. It is a desktop, yes.
Q. They are working on a desktop. And they are designing and they are configuring the GEMS databases, which basically determine how a voter's choice at that electronic string gets transmitted into the tabulations; correct?
A. They are constructing the database, yes, sir.
Q. Okay. And do you know what sort of security they have in their homes?
A. They are under the same purviews as we are in relation to their equipment, that it must be air gapped as our equipment

for ballot building purposes is. And they deliver -- hand-deliver those copies of databases to the Secretary of State's office for direct inspection.

Once those databases come into our possession, they are not then returned back to ES&S if any corrections or any issues are found within the database. All corrections to issues found are then corrected within our office, reviewed by members of my staff, and then images provided to direct counties for inspection.

Q. Do they have any particular physical security at their homes or garages where they are doing this work for the State of Georgia's voting system?

A. I don't know which -- I don't know what security parameters each individual has within their home.

Q. Okay. And do you recall the protocols that the Judge in this case approved for our experts' handling of the GEMS databases? Were you involved in that?

A. Only tangentially.

Q. Do you recall that it was in a special room at the University of Michigan with tight security and videotape? Do you recall all of those?

A. I do.

Q. Are any of those protections or security measures taken with respect to the three individuals who do not even work for the Secretary of State at their homes or garages while they are

locked USB drive?

A. It is a lockable USB drive, yes.

Q. And can you -- could you walk us through the process that you go through when you are taking data and putting it onto the USB drive.

A. Right. First off, start off with a drive. Verify that it has been formatted. I do that on my public-facing computer, my SOS public-facing computer. Format the drive. Once the drive has been formatted, then I remove it from the public computer and proceed to my private computer on the private GEMS system.

Then the data files are copied from the GEMS computer and placed onto the USB drive. The USB drive is then removed from the private drive and then placed into its locked position. It is then transferred -- pulled over to the public computer -- inserted into the public computer. And then the files are copied from that drive onto the public computer for distribution to counties.

Once that process is completed, then we unlock the drive and then format the drive.

Q. Now, when the drive is inserted into the internet-facing computer, is it -- do you know if it is scanned for malware at that point?

A. It is my understanding that the Secretary of State's office has a protocol in place that for any drive that is inserted it is immediately scanned.

MS. BENTROTT: Objection. Lacks foundation.

THE COURT: Is it an understanding based on -- do you have personal knowledge, or has somebody else told you that?

THE WITNESS: My Secretary of State's IT office has told us that every drive that is placed in whether it is --

THE COURT: All right. But that is based on some information they provided to you?

THE WITNESS: Yes.

THE COURT: You haven't been present? You haven't observed that yourself?

THE WITNESS: When I insert a USB drive, there is always something that pops up that gives us indication that something has taken place with that drive.

THE COURT: All right. So that is the basis of your knowledge?

THE WITNESS: Yes.

THE COURT: You don't have any personal knowledge from having participated in this over at the Secretary of State's office?

THE WITNESS: Correct.

THE COURT: All right.

Q. (BY MR. RUSSO) Do you know if there are any other restrictions that are in place on the Secretary of State's network for pulling -- when you want to pull data onto that USB drive?

A. Again, my understanding of what we have been educated by our IT office is that any time that a file is generated and generated by, say, for example, eNet -- when we have to pull data files from eNet for ExpressPoll purposes, that when that data file is built it is scanned for malware. And then when it is transitioned to a jump drive, it is then encrypted information. Because all data that comes off of the SOS public computers, that data must be encrypted in order to be moved.

MS. BENTROTT: Same objection, Your Honor. Lacks foundation.

THE COURT: All right. I'm going to strike that unless you can create a foundation.

Q. (BY MR. RUSSO) Is there anything that you need to click on your computer screen to --

MS. BENTROTT: Objection. Leading the witness.

THE COURT: All right. I just need him to explain what he -- the basis of his testimony.

MR. RUSSO: That is what I'm trying to ask him.

THE COURT: Just don't lead.

Q. (BY MR. RUSSO) Whenever he is trying to transfer files over, do you click on anything that indicates it has been encrypted?

MS. BENTROTT: Objection. Leading.

MR. RUSSO: Well, I'm asking him.

THE COURT: We're going through a lot of leading

questions. Just simply: What is the basis of your testimony as to the eNet data?

THE WITNESS: When I have copied data from my public computer onto a jump drive, if I take that jump drive over to my private computer, in order to -- in order for the data to be read by my private computer, I first have to put in a password on my jump drive that allows access to the data.

THE COURT: All right. So you understand that that -- that is the system at least relative to your experience of it?

THE WITNESS: If I -- I first have to put a password in to access the drive. Once I have accessed the drive, I actually have to launch an executable within the folder. If I don't launch the executable within the drive folder, if I just move the file over, just literally drag it, it is unreadable.

So that is my understanding of it being encrypted. That I actually have to run a process to launch the decryption.

THE COURT: Do you know that that is the process for anyone else or not?

THE WITNESS: That is the process for all SOS employees when moving data from the public computer to any other computer.

THE COURT: Okay. Does this -- are these eNet files also sent to county personnel?

THE WITNESS: County election officials have access

to eNet. But the data files that I'm speaking of are the data files that are used to produce the electors' list that is seen on ExpressPoll within the polling location.

THE COURT: Go ahead.

Q. (BY MR. RUSSO) Mr. Barnes, are you familiar with the state's contract with ES&S for ballot building?

A. I am.

Q. And do you know if that contract has any security measures in it to ensure that the ballot building process follows the state's current procedures?

A. I believe it does.

MR. RUSSO: No further questions, Your Honor.

THE COURT: Have you reviewed the contract?

THE WITNESS: Yes, ma'am. I believe it is about four or five pages in length with a very detailed section in relation to what security requirements they are to uphold.

MR. RUSSO: Thank you.

THE COURT: Could I just ask a few questions that are follow-up. And, again, they don't count against anyone. And take a minute for my questioning as it is off beforehand.

EXAMINATION

BY THE COURT:

Q. Do you have any familiarity with the contract between the Georgia Secretary of State's office and PCC?

A. No, ma'am, I do not.

Q. And are you involved in the voter registration database at all?

A. I have access to the voter registration database in order to obtain files to build the electronic data set for ExpressPoll, but I do not work in the voter registration division.

Q. All right. But the data from the -- that is being manipulated or in the past was manipulated on the software and operations of PCC, would that be transferable then to the Secretary of State's office?

A. I do not know.

THE COURT: All right. Thank you very much.

MS. BURWELL: No questions, Your Honor.

MS. BENTROTT: Some redirect, Your Honor.

THE COURT: All right.

RECROSS-EXAMINATION

BY MS. BENTROTT:

Q. Thank you, Mr. Barnes. When you plug the USB drive into your public-facing computer to reformat it, you have to unlock the USB drive; correct?

A. After I have placed the locked drive into the computer to move -- copy the files over, I then remove the unlocked drive -- I remove the locked drive, switch it to unlocked, reinsert the drive back into the public computer, and then do my formatting.

Q. And that is true for the USB drive that you plug into the GEMS servers; correct?

A. That is the -- yes. It is formatted on the public side before it is placed back into the private side.

MS. BENTROTT: Thank you. Nothing further.

THE COURT: May this witness step down?

MR. BROWN: No further questions, Your Honor.

THE COURT: Thank you very much.

I just want to get back again to the contract between the Secretary of State's office and the PCC. I don't know whether the contract that just renewed is the same contract other than date frame as the one that was reviewed in the cyber risk assessment of 2018. But if it is the same other than the time frame, I don't need to see the one that was looked at in 2018. But if it is a different one, I'll need both.

MR. TYSON: Okay. And, Your Honor, on that point, in communicating with the Secretary of State's office, there are some changes regarding the hosting obligation. So it will be different. But the belief is that the auditing functions were included. So we're going to go ahead and get that for you.

THE COURT: Okay. Thank you very much.

MR. BROWN: Your Honor, Bruce Brown. We were going to -- I was going to reference this in my opening. But this relates to the testimony of Mr. Barnes. With your permission, we're going to serve and file a hearing brief on evidentiary

THE COURT: What was the letter? What was the exhibit number or letter of the affidavit?

MS. BURWELL: Her affidavit is Document 277 starting at Page 93.

THE COURT: Okay. It is not in this group. All right. Thank you.

Do you remember what the mid level price was?

THE WITNESS: Twenty-six cents per ballot.

When you -- and this is something that we did when we transitioned. But when you factor in the cost of, you know, less equipment, less delivery, all of that, coupled with the cost of the ballot printing, you actually see more of a savings when you are not having to have as much equipment out in the field and process all of that out in the field. So it varies. But we saw a savings.

THE COURT: All right. Thank you.

MR. BROWN: I just have one follow-up question, Your Honor.

REDIRECT EXAMINATION

BY MR. BROWN:

Q. You testified that you saw some savings. And just so the record is clear, you saw some savings in the transition from DREs to hand paper ballots? Is that what you meant?

A. Yes. So we no longer needed a warehouse. We had a 40,000-square-foot warehouse where we had DREs that went away.

THERESA PAYTON,

after having been first duly sworn, testified as follows:

CROSS-EXAMINATION

BY MR. CROSS:

Q. Good afternoon, Ms. Payton.

A. Good afternoon.

Q. Do you consider yourself an expert on election security?

A. Yes, Your Honor, I do, on certain aspects of election security.

Q. Specifically involving cybersecurity in elections?

A. Yes.

Q. And --

THE COURT: What aspects do you not feel like you're an expert on?

THE WITNESS: Well, it will depend as we go into sort of the context of different parts of it. But as it relates to cybersecurity, pretty much any hardware or software and sort of oversight of a process, we look at that at Fortalice Solutions, whether it is election security or any other process.

Q. **(BY MR. CROSS)** Ms. Payton, as someone with some expertise in election security, your biggest worry and concern going into the midterm elections of last year was that citizens would not trust election results and that the election process would lose legitimacy; right?

A. That is correct. I'm actually working on a book that I've

been working on the better part of two years around -- I call it sort of the security of the ecosystem, everything from campaigns, to the party headquarters, to how the different states run things in the elections, as well as the manipulation that occurred on social media.

Q. And going into the midterm elections of last year, you had grave concerns about election interference; correct?

A. I did, yes. Still do.

Q. In fact, going into the midterms of last year, you believe that one thing that we can be sure of is that a U.S. election will be hacked, no doubt about it; right?

A. Yes. Now, as far as kind of --

THE WITNESS: If you don't mind, Your Honor, I would like to give a little bit more context if you want it or I can give more context later.

MR. CROSS: Since it is on my time, I would rather her just rely on redirect.

THE COURT: That is fine.

THE WITNESS: Sure.

MR. CROSS: Thank you, Your Honor.

Q. **(BY MR. CROSS)** Did you watch any of the Congressional hearings with Robert Mueller?

A. I listened to it first thing in the morning on the way in to work. You mean the one that occurred this week, sir?

Q. Yesterday.

Q. In fact, you have praised Wisconsin for the fact that it uses paper ballots; right?

A. Yes. In the op-ed, that is correct.

Q. In the Georgia system, you mentioned a running print. There is not actually a running print? There is just the single total at the end; right?

A. That is -- as I understand it from the demonstrations I have seen, yes.

Q. Now, you agree that suppressing even a relatively small handful of votes, particularly in a local election with a small number of voters, could be enough to change the outcome of an election; right?

A. It is possible. You certainly don't want a single vote suppressed.

Q. And you are aware of cyber attacks in 2018 on the infrastructure that could actually suppress voter turnout in the U.S.; right?

A. There is the possibility.

Are you referring to Illinois or a specific event or just in general?

Q. Well, you're aware that in 2017 and 2018 security researchers discovered that Russian hackers were probing the U.S. electrical grid?

A. That is correct. Department of Homeland Security and others went out to talk to the states that had those probes.

assessments, including whether any attempts to penetrate systems have been successful. If you need to take a look at that, go ahead.

A. Uh-huh (affirmative).

Q. So we've heard a lot about it. But just to lay the groundwork, you conducted, your team, three assessments in 2017 and 2018, one in October '17, one in February of '18, and one in November of '18, for the Secretary of State; right?

A. That's correct.

Q. So the assessments you are talking about here in Paragraph 4 -- you are talking about those assessments in looking for attempts to penetrate -- to see whether penetrate systems have been successful; right?

A. Uh-huh (affirmative). Yes.

Q. Just so we are clear, that work did not include examining GEMS servers, DREs, memory cards, scanners; right?

A. That is correct.

Q. So I gather you were not engaged to do that analysis for your declaration either; right?

A. That is correct.

Q. Or for those three risk assessments; correct?

A. Correct.

Q. In Paragraph 4 of your declaration, you say that the risk assessments included an attempt to isolate malicious activity; right?

A. Yes.
Q. You did not conduct that analysis for the purpose of those risk assessments or your declaration with respect to GEMS servers, DREs, memory cards, or scanners; correct?
A. That is correct.
Q. You could have, but you were not engaged to; right?
A. That is correct. They -- it was a different focus and a bigger part of the ecosystem.
Q. In Paragraph 4, you also point out that your risk assessments included an attempt to determine where any malicious activity originates; right?
A. Yes.
Q. And as with the other, that assessment did not include GEMS servers, DREs, memory cards, or scanners; right?
A. Correct.
Q. You could have done it, but you were not engaged for that; right?
A. Correct.
Q. You participated -- strike that.
So let's talk about the October of 2017 assessment, which is Exhibit 1. If you need a copy of it, let me know.
A. I would like to have it.
Q. Sure.
A. We write hundreds of reports every quarter. So I would just like to have it.

Q. I understand. Are the exhibits still up on the stand? It may be in front of you. It is Exhibit 1.

THE COURT: I think it is going to be larger than that.

COURTROOM DEPUTY CLERK: Mr. Beaver took the exhibits when he left.

MR. LAKE: We may have it. Which one are you looking for?

THE COURT: Exhibit 1.

THE WITNESS: I don't have it.

THE COURT: He was ready to leave.

MR. CROSS: He was eager to get out.

Thanks, Bryan.

MR. TYSON: How many do we need?

MR. CROSS: Just one for her.

May I approach, Your Honor?

THE COURT: Yes.

Are you handing her a redacted one or not redacted?

MR. CROSS: This is unredacted just for her so she has full context.

Q. (BY MR. CROSS) So, Ms. Payton, you have what has been marked as Exhibit 1. And this is a copy of the assessment that your team prepared in October of 2017 for the Georgia Secretary of State; right?

A. Yes.

Q. And your team assessed the Secretary of State IT security as Tier 2 on the NIST scale? I think you mentioned NIST a moment ago; right?

A. Yes, sir.

Q. What that means is that awareness of cybersecurity risks -- that they had an awareness of cybersecurity risks at the organizational level but an organization-wide approach to managing cybersecurity risks had not been established. That is what that meant; right?

A. That is what it means, yes.

Q. And your team at that time identified 22 security risks in the Secretary of State's IT operations; correct?

A. We did.

Q. And you characterized most of those as significant risks; right?

A. We did.

Q. One of those risks was widespread local administration rights or administrative rights; correct?

A. That's correct.

Q. And that meant that all Georgia Secretary of State users who had any sort of log-in credentials were granted administrative rights on their work stations; right?

A. Yes. In some cases, yes.

Q. And by administrative rights, that means they have the ability to, for example, download software; right?

A. Yes. If they know that is there. Not all users do.
Q. You understood -- in fact, advised the Secretary of State that this increased the likelihood that malware or a malicious actor would be able to successfully compromise a user's work station through email, web, or removal of media?
A. Yes. It is one of the first things we look for. This is actually pretty common to see this vulnerability in private sector firms and government organizations.
Q. Ms. Payton, the problem was particularly acute at the Georgia Secretary of State though because users not only had administrative rights on their own work stations but they had -- any individual users had administrative rights on all work stations? You found that; right?
A. In some cases, yes.
Q. This meant that an attacker who took advantage of having access to the administrative rights could -- with access to a single work station could quickly access any other work station and gain administrative rights to spread malware, install remote access tools, or access sensitive data? That is what you found; right?
A. Yes.

Do you want some context, or you just want yes or no? I just want to be respectful of your time.

Q. I appreciate that. I'm on the clock, and there are a lot of really smart people across the aisle that will have lots of

good questions for you.
A. Okay.
Q. Another risk you identified was the lack of two-factor authentication for remote access; correct?
A. Yes. That is correct.
Q. And that meant that the Georgia Secretary of State users were able to remotely access the Secretary of State network using only a user name and a password?
A. At that time, yes.
Q. And best practice, even as of this time, was to go to at least a two-factor authentication? You recommended that?
A. Absolutely. Two-factor whenever you can do it.
Q. You found that this level of security was insufficient, particularly given the possibility of fishing attacks or the theft of credentials; right?
A. Yes.
Q. And this particular vulnerability involves remote access -- people remotely accessing their Secretary of State accounts outside of the office; correct?
A. Yes. This is something we very commonly find in many organizations.
Q. Did you hear today that the Secretary of State relies on individuals to design and develop GEMS databases working out of their personal homes?
A. I did not. I don't think I was here for that, sir.

Q. Have you ever heard that before today?
A. I had not.
Q. So that is not something you evaluated for your risk -- either of the three risk assessments; right?
A. No. That is correct.
Q. That is not something you evaluated for your declaration; correct?
A. Correct.
Q. Another risk that you identified was the use of nonunique local administrator passwords; right?
A. That is correct.
Q. And that risk you advised the Secretary of State could allow an attacker who compromises one work station on the network to obtain the local administrator account credentials and then use those credentials to gain access to any other work stations or servers; right?
A. Yep. Again, this is a common attack vector that we see attackers take. And it is something we very commonly see as a deficiency in organizations.
Q. You keep saying that. But let's be clear. Nowhere in your declaration do you state that the risk factors that you have identified -- that those are present in the election systems or in any way in the Secretary of State's office of any other state? That does not appear in your declaration; correct?

A. Correct.
Q. That also does not appear in any of the three assessments that you did for the Secretary of State; correct?
A. What doesn't appear?
Q. That the risk factors that you have identified, that each of those -- let's just take 2017. That the 22 risk factors you identified, that you had conducted a similar analysis of a Secretary of State and found the same risk factors? That does not appear in your assessments?
A. That is correct. It does not.
Q. On the one we were just talking about, nonunique local administrator passwords, when you did your third assessment, which completed November 30 of 2018, you found that that one was still present; right?
A. We did. It is very common. It is hard to get things fixed. And sometimes the fixes break other things. So that is why sometimes it is a little bit more complex than just turning it on.
Q. But you did recommend in October of 2017 that they fix that?
A. Yes, we did.
Q. So by the time we got beyond the midterm election of 2018 where 4 million voters in the State of Georgia voted, you found that that assessment -- that risk was still present; correct?
A. That's correct. What I can tell you is these roadmaps

when we -- first of all, we get paid to find things. That is our job. But secondly --

Q. Ms. Payton, I promise you are going to get an opportunity to explain from them.

A. Okay.

Q. So we have the timing right, the 22 risks -- your team identified these 22 risks and successfully even penetrated the Georgia systems as reflected in your October 2017 report; right?

A. Yes.

Q. And this occurred after it was widely publicly known that Russia had attempted to interfere in the 2016 elections; right?

A. It was becoming more publicly known at that point. Yes.

Q. So then for the February 2018 assessment, that one focused on the PCC technology which at that time owned and operated the voter registration database; right?

A. Yes. That is correct.

Q. And they continued to own and operate the registration database through the midterm elections of last year; right?

A. Yes.

Q. In fact, we heard today I think that only recently until July of this year has there been efforts undertaken to switch that and to give some more authority to the Secretary of State's office? Had you heard that?

A. I was not in the room for that.

Q. In the February 2018 assessment, you identified 15 security risks with PCC involving the voter registration databases; right?

A. I believe that is correct. I'm trying to flip -- do you -- do you know where it is in here? I just want to make sure.

Q. I think it is right in the front of the February assessment. I think it is on the first page.

A. This is a thick document. So hold on a second. Let me --

Q. Do you have the February one up there, or do you need that one too?

MR. TYSON: We have the February one.

THE WITNESS: Yeah. I just have the 2017.

MR. CROSS: May I approach?

THE COURT: Yes.

A. What page are you on?

Q. **(BY MR. CROSS)** I think it is the first. Let's see. If you look at the second paragraph, you see it reads --

A. On Page 3?

Q. First substantive page, Page 3. Are you there?

A. Yes.

Q. Thank you. It reads, Cloudburst Security suggests remediating the 15 identified security risks included in this report. Do you see that?

A. Yes, I do.

Q. So does that refresh your recollection that as of the February 2018 report your team had identified 15 security risks with respect to the PCC and the voter registration?

A. Yes.

Q. As part of the assessment you did, you actually reviewed the contract between the Secretary of State's office and PCC; right?

A. Yes.

Q. And you found that the contract did not contain any cybersecurity requirements at all; correct?

A. Yes. Also common oversight.

Q. But, again, there is no indication in this report that the Secretary of State didn't need to take that seriously because it just happens all over the country? That doesn't show up in there; right?

A. Just because it happens other places doesn't mean I don't take it seriously or tell my clients not to.

Q. Thank you. That would be the point.

You found that PCC was relying on outdated software that was known to contain critical security vulnerabilities; right?

A. Correct.

Q. You noted that an attacker with sufficient time and resources could exploit those vulnerabilities; right?

A. Yes.

Q. You identified certain remote access vulnerabilities as

well; right?
A. Yes.
Q. In particular, PCC did not block VPN connections from IP addresses of known threat sources or foreign countries; right?
A. Correct.
Q. And you identified a number of missing critical operating system patches, unsupported software, and vulnerable third-party software; right?
A. Correct.
Q. Then you did a third assessment that was between September and November 30 of 2018; right?
A. Yes.
Q. That actually --
A. May I have a copy of that just to be on the safe side?
Q. Yes, ma'am.
A. Thanks. Thank you.
MR. CROSS: I'm afraid Mr. Tyson is going to hand me -- he is going to trick me here and give me something I shouldn't show you.
Q. **(BY MR. CROSS)** So you have that one in front of you?
A. Yes, I do.
Q. And based on the assessment that you did that ended on November 30 of 2018, you made 20 additional recommendations to the Secretary of State to improve their cybersecurity; right?
A. We did.

Q. And according to your declaration -- I think it is Paragraph 7 if you want to grab a copy.

Do you have that in front of you?

A. Yes.

Q. Of the risks outlined in the 2017 report, your team found that as of the November 30, 2018, reassessment, you say three risks have been remediated with compensating controls; right?

A. Yes.

Q. So 3 out of the 22 that you had identified in 2017 had been remediated as of November 30; right?

A. Yes.

Q. And another three were in process; right?

A. Yes.

Q. Meaning that as of November 30, weeks after the midterm election, your team found that of the 22, 19 had not been remediated at all; right?

A. Correct.

Q. And 16 were not even in process; right?

A. That's correct.

Q. So you weren't here for Mr. Beaver's testimony, I believe you said?

A. No.

Q. Mr. Beaver testified that he thought you were wrong about that. So I'll ask you: Were you careful when you prepared your declaration?

A. Yes.
Q. Were you careful when you conducted these assessments?
A. Yes.
Q. Did you adhere to professional standards when you conducted each of these assessments?
A. Yes.
Q. Did you follow the scope of the work as it was laid out for you?
A. Yes.
Q. And were you honest and accurate in the declaration you provided here?
A. Yes.
Q. As you sit here today, do you have any reason to believe that you're mistaken, that your team was wrong in saying only 3 of the 22 risks had been remediated as of November 30, 2018?
A. I stand by what I have in my affidavit.
Q. And when you prepared the November 30, 2018, risk assessment, did anyone at that time from the Secretary of State's office say to you, you've made a mistake, we have actually remediated more?
A. No.
Q. And since you prepared your declaration, has anybody on behalf of the state told you that your declaration was wrong in any way?
A. No.

Q. We talked earlier that you mentioned NIST. You actually provided a numeric score to Georgia Secretary of State as part of your November 30, 2018, assessment; right?

A. Yes.

Q. And that score ranges from 0 to 100; right?

A. Which score?

Q. Well, you gave them --

A. Are you talking about the NIST score or the risk weighting model that we use?

Q. It is the one -- if you look at the bottom, you see there on the report it has your name and then there is a little series of numbers, Payton and then zero zero zero.

A. Uh-huh (affirmative).

Q. Look at the one that ends in Page 112, if you will.

A. 120?

Q. 112.

A. I'm sorry. I feel dumb. I don't know what -- oh, you mean from 2017. And then I'm looking for 112?

Q. Yes. Sorry.

THE COURT: Are we talking about 112 in the 2018 report?

MR. CROSS: Yeah. The 2018 report.

THE COURT: The November 2018?

THE WITNESS: Sorry.

MR. CROSS: The one you had.

THE WITNESS: I'm sorry.

MR. CROSS: It is Page 43 of your report, if that makes it easier.

THE WITNESS: Yes. Thank you.

Q. **(BY MR. CROSS)** So here you have -- there is a chart, and you give them a score based on your overall assessment; right?

A. Yes.

Q. And that score is between 0 and 100; right?

A. That's correct.

Q. What is good? 0 or 100?

A. 100, just like grade school.

Q. I figured. The score you gave them was only 53.98 on your overall assessment; right?

A. Correct. It is a little different -- well, I'll just say correct.

Q. Thank you.

A. Save you the time.

Q. You are very kind.

In October of 2017, your team expressed -- going back to October '17, your team expressed an overarching concern for the lack of control and oversight the state was able to maintain over the voter registration database; right?

A. Correct.

Q. In February 2018, you identified, as we discussed earlier, 15 security risks involving the same registration databases;

Q. I think so. If you start on 191 -- just so we're clear, look at the bottom of 191. Do you see it indicates that these are the notes of the interview with Chris Harvey?
A. Yes, I do see that. Yes.
Q. Do you see in the middle where you were looking -- do you see in all caps who hosts it? Do you see that?
A. Yes.
Q. The answer is PCC vendor from 2012. Do you see that?
A. Yes.
Q. And to get there, again, we're talking about the voter registration databases; right?
A. Yes. That's correct.
Q. And Mr. Harvey indicated at this time that, being the voter registration databases, that is what Russian hackers would want to get into? Do you see that?
A. Yes.
Q. So that was -- that feedback was at least among the factors that you and your team considered in advising the Secretary of State to remediate the risk that you found with the voter registration database at that time; right?
A. Yes.
Q. You then did your November 2018 assessment. But at that point in time having looked at the voter registration database twice before and found a number of risk factors, by the time we get to the timing of the midterm elections, the Secretary of

State directed you that PCC and the voter registration database was out of scope for the November 2018 assessment; correct?

A. Yes.

Q. So we're clear, for the November 30, 2018, assessment, coinciding with the midterm elections, you did not conduct an assessment of PCC or the voter registration databases in the way that you had for the prior reports?

A. Correct.

Q. Do you recall that your team interviewed Lorri Smith, the chief operating officer?

A. I do. I don't remember the notes exactly.

Q. I can direct you if you need it. But do you recall that she informed your team that she thought the state's weakest link is their employees?

A. That is actually a common saying of the cybersecurity industry, that the human is the weakest link.

Q. That was one of the things you heard here; right?

A. I didn't hear it here. I wasn't here for --

Q. Your team did?

A. During the interviews?

Q. Yes.

A. Yes. Yes. I mean, Secretary of State of Georgia was incredibly candid and critical of themselves throughout the interviews.

Q. Which, again, is what helped you identify 22 risks in

A. I wouldn't want to run my stuff on it. But you can get -- you can pay for patches. The banks are paying for patches for ATMs.

Q. You anticipated where I was going.

Are you aware that from the evidence we have seen the last patch to the current election system using GEMS and DREs is from -- at least for GEMS, I think, is 2005?

A. No. I was not aware.

Q. You did penetration testing in November 2018 that successfully gave your team administrative rights over the Secretary of State's domain; right?

A. Correct.

Q. You talked about your Fortune 500 clients today. And I don't want to reopen a door. But since the judge allowed some of that, I just briefly want to touch on it.

But just so we are clear, you are not offering an opinion in this case that the same level of security that would be appropriate for, say, a Fortune 500 company dealing with their own private data -- you are not offering an opinion to the Court that that would be appropriate security for managing an election and election data and election equipment; right? That is not an opinion you have offered in this declaration; right?

A. I have not offered that in the declaration. That is correct.

Q. The risk assessments you did, that was only for the

Secretary of State; right?
A. And the vendor.
Q. And the vendor?
A. Yes.
Q. You didn't do a similar risk assessment for any of the 159 counties in Georgia; right?
A. That is correct.
Q. So in looking at the vulnerabilities -- cybersecurity vulnerabilities, you did not assess the degree to which each of the counties, for example, having their own GEMS servers -- what vulnerability that might present for the Secretary of State; right?
A. That's correct.
Q. Are you aware that county election servers are connected to phone lines using modems? Was that something you knew?
A. We did not look at that architecture.
Q. Were you here for Mr. Barnes' testimony?
A. Part of it, I believe. I came in towards the end of somebody's testimony. I'm sorry if I -- I think it was Mr. Barnes.
Q. Are you aware that Mr. Barnes testified today and then again in September of last year that he has a USB drive he plugs in to his public-facing computer, which means he is connected to the internet, and then he plugs that same USB drive into what he calls an air-gapped GEMS server? Do you see

C E R T I F I C A T E

UNITED STATES OF AMERICA

NORTHERN DISTRICT OF GEORGIA

I, SHANNON R. WELCH, RMR, CRR, Official Court Reporter of the United States District Court, for the Northern District of Georgia, Atlanta Division, do hereby certify that the foregoing 312 pages constitute a true transcript of proceedings had before the said Court, held in the City of Atlanta, Georgia, in the matter therein stated.

In testimony whereof, I hereunto set my hand on this, the 2nd day of August, 2019.

Shannon R. Welch

SHANNON R. WELCH, RMR, CRR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT